ADMINISTRATIVE DIRECTIVE NO. 7.3

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES

1. PURPOSE:

This directive establishes policy and fixes responsibility for ensuring the security, privacy, and confidentiality of data maintained by City departments in computerized systems.

2. RESPONSIBILITIES:

A. The Information Resources Department shall be responsible for developing, maintaining, publishing and administering a comprehensive **DATA SECURITY PLAN.** This plan shall reference applicable statutes, ordinances and Administrative Directives pertaining to Data Security. At least industry standards for security, integrity and recovery shall be adopted and strictly enforced. The plan shall be applicable to remote sites or facilities in all City offices or spaces and shall ensure that unauthorized access to City data processing resources is prohibited. The plan shall include audits and intrusion detection procedures.

B. The Information Resources Department, through its Data Administration function, shall serve as the contact point and coordinator for data sharing among City departments and dissemination of data on magnetic media to the public and other agencies.

D. The Owner of the Data shall be responsible for:

Determining the sensitivity classification for all data.

Establishing procedures for dissemination of data to the public from computerized systems for the Owner's department in compliance with Administrative Directive 1.31, Open Records.

Approving or developing procedures for backup and recovery.

Approving on-line access by other users.

2. RESPONSIBILITIES: Cont'd)

Developing an availability impact statement for all computerized systems. This statement will briefly outline the impact on the department's operation if the computer system supporting a function is inoperative.

Establishing and enforcing procedures designed to insure the integrity of the data contained in computerized files.

Approval and responsibility for all software developed or procured from any source other than the Information Resources Department.

D. The User is responsible for:

Safeguarding the City's data resource.

Complying with the provisions of the SECURITY PLAN and relevant Administrative Directives.

3. POLICY:

A. The data and information in the City's computerized systems, along with the hardware and software required to process the data, are a valuable resource and represent a significant investment.

B. All reasonable precautions shall be taken to insure the security of the data and of the software; and to protect the privacy and confidentiality of the data while allowing reasonable access and dissemination policies which are consistent with applicable statutes, ordinances and directives.

4. APPLICABILITY:

For the purpose of this Directive, the following are deemed to be the property of the City of San Antonio and are subject to the provisions of this Directive:

4. APPLICABILITY: (Cont'd)

A. All computer hardware, Data Communications devices of whatever nature, procured with City funds, residing on City property or used in the conduct of City business.

B. All software, firmware or other data processing entity, system description, program description, software documentation or other documents developed by City personnel or with City funds or licensed to the City of San Antonio.

C. All data from whatever source and in whatever form which is entered into, stored by, processed by or retrieved from or through any City computer.

5. DATA CLASSIFICATION:

All data shall be classified as Public, Operational, or Confidential for the purpose of establishing dissemination guidelines. Administrative Directive 1.31 places responsibility for developing and updating the Municipal Open Records Policy and Fire and Police Open Records Policy with the City Attorney. This responsibility includes responding to requests for opinions on whether or not records are public under the Open Records Act. Classification of data shall conform to those guidelines.

A. CONFIDENTIAL DATA

Data in this classification is that which may not be disseminated or which has restricted dissemination, mandated by Statute, Ordinance, Court Order or Directive.

B. OPERATIONAL

Data which is specifically exempted from the Texas Open Record Law.

C. PUBLIC

All data and information not classified as CONFIDENTIAL or OPERATIONAL.

6. DISSEMINATION GUIDELINES:

A. PUBLIC DATA

This data may be disseminated to anyone requesting the data as follows:

The Owner, or designated employee, of the data may disseminate the data or information derived from the data to anyone. Fees may have been established by ordinance for this service.

All City departments may have access to this data. However, the requesting department shall submit a request in writing to the Data Administrator who will notify the Owner and insure the operational integrity of the data.

All requests for data to be provided on magnetic media shall be made to the Data Administrator. The Owner of the data will be notified in writing of the request and be informed of the data provided and to whom it was provided.

All requests for copies of software, program descriptions, system descriptions or other computer related documentation shall be made to the Data Administrator who will maintain a list of such disseminations.

B. OPERATIONAL DATA

Data in this classification usually consists of incomplete work products of the City and other data which is exempt from the Open Records Law. The following rules apply:

No employee shall disseminate data in this classification without authorization from the Department Head or City Attorney.

This data may be shared with other City departments. However, the requesting department must submit a request to the Data Administrator. If the Owner agrees to share the data, the Data Administrator will insure that adequate protection for the data is in place.

6. DISSEMINATION GUIDELINES: (Cont'd)

B. OPERATIONAL DATA (Cont'd)

Systems shall be designed in such a way as to insure the privacy of data within this classification.

C. CONFIDENTIAL DATA

Data within this classification usually consists of data which is prohibited from disclosure by statute, court order or decision, ordinance, or Administrative Directive, and is generally that which would violate the rights of citizens or compromise the City in fulfilling its obligations.

This data may not be disseminated by any employee.

This data may not be shared with other departments, except by written authorization by the City Manager.

The Data Administrator shall insure that extraordinary procedures are employed to protect the confidentiality of this data.

7. PROHIBITIONS:

A. No employee shall use anything subject to this Directive for personal gain.

B. No employee shall intentionally or knowingly access or attempt to access any City data without having both the right and the need to access such data.

C. No employee shall add, update or delete or attempt to add, update or delete any record or data within any data file, data base or system without having a legitimate City business need and proper authorization to do so.

7. PROHIBITIONS: (Cont'd)

D. No employee shall disseminate any data subject to this Directive unless such dissemination complies with the guidelines in paragraph 6.0.

E. No employee shall make any copy of any software, system documentation, program description or any other descriptive material for dissemination unless such dissemination complies with the guidelines in paragraph 6.0.

F. No employee shall procure, obtain or use in any manner any software developed by non-City personnel, or any City computer without having the proper licenses and approval from the Owner of the Data and the Department Head having custody of the computer.

G. No employee shall discuss the details of the SECURITY PLAN or disclose any program name, access code, user identification, password, telephone number or any other item of information that may compromise the City's Data Processing Resources or Data.

H. No employee shall knowingly permit any other person to violate any provision of this Directive.

8. PENALTIES:

Violation of any of the Prohibitions outlined in Section 7 above, shall result in disciplinary action. Administrative action may range from a reprimand and loss of access privileges to termination of employment. Violations may also result in civil and/or criminal prosecution.

9. DEFINITIONS:

A. DISSEMINATE - to communicate, by any means, information of any kind to any person or entity who is not authorized to directly access the information at its source.

9. DEFINITIONS: (Cont'd)

B. **OWNER** - The department or other organization responsible for creating and maintaining a specific item of data.

C. **USER** - Anyone who has access to an item of data from any City file or has access to any other CIty Data Processing resource.

APPROVED:

FRANK A. STROMBOE, Director
Information Resources Department

LOUIS J. FOX, City Manager
City Manager's Office